Smart Mobile Attendance System using Bluetooth technology

Ankit B Dubey[1], Nitesh Gupta[2], Ankit M Dubey[3], Nilima Nikam[4]

[1,2,3,4]*Student,Dept. of Computer Science and Engineering,YTIT college, Karjat, India*

Abstract—*This paper provides an idea for smart attendance management system using Bluetooth. In the current scenario of companies and colleges attendance is marked using various RFID card, biometric systems and in some places, manually. The proposed system in this paper uses Bluetooth technology provided in cell-phones an application to mark attendance and employee tracking in company premises. The system identifies the potential use of Bluetooth and Database to keep employee's and student records and to efficiently store and retrieve the same for evaluation. An Bluetooth-supported College M-Attendance system for University Students is discussed as one potential use of this technology. The proposed framework replaces manual roll calls and hence, making it resilient to forgery. It gives parents and professors information about the students' attendance. The marking of attendance is quick, unsupervised, and makes use of a One Time Password (OTP) to enhance the security of the system and takes away the possibility of proxy attendance. Bluetooth as a technology that is more secure and convenient than the prevalent technology of biometric, and also elaborates on the proposed framework of the M-Attendance system that makes use of this advantage that Bluetooth has over other technologies.*

Key words: One Time Password, Attendance, Student, Bluetooth Smart

I. INTRODUCTION

Bluetooth and one time password (OTP) upheld M-Attendance structure for little scale association. Traditionally employee needs to maintain the enrollment records for participation. This routine requires time and exertion, compromising on the working time. Expansion to this, a few employees exploits the benefit of low-security attendance framework and test the participation of the representative who is not available in the office [8]. The proposed M-Attendance framework has been intended to design to simplify streamlines attendance monitoring. It replaces the standard attendance checking framework and makes it faster, more secure and totally advanced.

Bluetooth is an industry wireless specification standard for use in various devices for short range communications. As a radio based technology it allows devices to share information over a maximum range of 10 meters. It has several applications in Mobile Communications and transactions. An Bluetooth supported college M- Attendance system for University students is discussed as one potential use of this technologyand reader into a solitary device. It permits clients to continuously share content material among advanced gadgets. A one-time password (OTP) is a password that is valid for only one login session or transaction, on any digital device. OTPs avoid a number of shortcomings that are associated with the traditional password based authentication systems. [2] The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. OTP systems also aim to ensure that a session cannot be easily intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus, reducing the attack surface further.

A. Abbreviations and Acronyms

TABLE I. ABBREVIATIONS AND DESCRIPTION

Abbreviation	Description
OTP	One Time Password
RF	Radio Frequency
SMS	Short Message Service
RFID	Radio-Frequency Identification

II. RELATED WORK

The purpose of SRS report is to list the customer or client requirement in a systematic way. It characterizes all the constraints and software requirement that are necessary to understand the application and documentation.

Functional Requirements

A functional requirement is nothing but what quality of work has been used in our system. Work is described as arrangement of input, behavior and output. Functional requirements are supported by non-functional necessities which force limitation on the plan or execution [7].

In this system we having two applications one is a web application in our architecture. Another application is android application which is developed using android SDK tools. The web application has following applications.

1. Admin Application: It is responsible to store the data on the server using database by providing employee or student details.

2. Employee's Application: Authorized employee's can login and mark his attendance can add his information in database.

3. OTP Message Service: If employee is an authenticated user OTP message will be sent to the user by admin.

Non Functional Requirements

The non-functional requirements of the proposed system are as follows:

1. Performance:
The framework will be utilized by many employees simultaneously. Since the framework will be facilitated on a solitary web server with a single database server in the background, Performance turns into a major concern.

2. Scalability:
The framework is sufficiently versatile to include new functionalities at later stages. There should be a typical channel, which can accommodate the new functionalities.

3. Reliability:
The proposed framework will be reliable; it will not give false positive results and the fake user such that one cannot rely on it.

4. Flexibility:
The proposed system will be flexible to the user with less complexity and user friendliness.

III. SYSTEM DESIGN

The system design includes various phases of project design which consist of description of project, algorithms and some high level diagram such as data flow diagram (DFD), sequence diagram, use case diagram and class diagram.

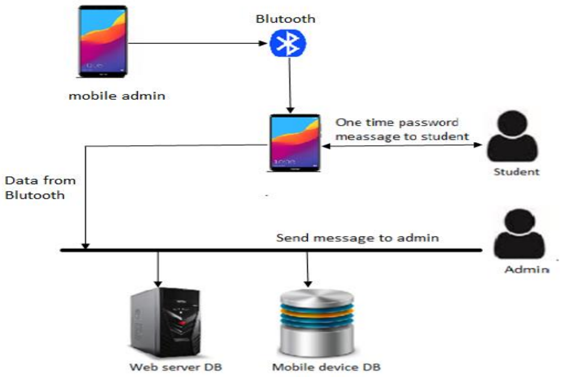


Fig -1: Architecture Diagram

Description:

The system design is a conceptual model which describes the structure, behavior of a system. The above 3.1 shows the system architecture which has the following steps.

Step 1: Admin login by using his Id and Password. Once the login is successful then he will write the employee details in the database and now it will contain the details of the employee.

Step 2: Employee/student uses ID and Password to login then they make Bluetooth on for attendance purpose. One time password will be generated for each employee by admin.

Step 3: Generation of one time password message and employee /user enters those OTP in the user's application, if password matches than user is an authenticated employee/user .If wrong OTP is entered or password entered doesn't match then user is not an authenticated employee/user.

Step 4: Once verification is successful it sends the time-in or time-out details to Admin by Professor. Admin gets time-in or time-out details of an employee. If the verification is not successful it displays invalid user.

IV. Working Module

A. Bluetooth

a. Writing the details student and professor in database

Once the registration of student is done then all data is stored in database by admin. Student can login whenever they required and can view their attendance and can mark their attendance. Same way professor can login and mark the attendance of the student using mobile device

b. Reading the data from Bluetooth device

Once the student is login to page and then can he search the device of professor for connection purpose. Once the connection is established then student wait for professor response. Professor login to page and select the device which he want to mark attendance and set the time and date of lecture.

c. OTP Verification

Once the professor mark the attendance then it goes under the verification stage where admin send the code via email which is OTP (mixture of alphabet and numeric caps and small) to student. Then he enter the OTP and attendance is confirmed by professor.

V. SECURITY FEATURES

The server in this system is the XAMPP server with PHP at its back-end. XAMPP needs to be configured to port number 80 so that the Apache server is able to receive requests from the localhost URL. The PHP code along with the SQL DDL command need to be added inside the htdocs folder. The exact location is "C:\xampp\htdocs". The back-end database should be intranet because admins located in the premises should be able to access the database as there is confidential information at stake. [11] Once the Tag ID is detected when student enters the class, the server is responsible for generating a random four digit number as OTP. As this number is a 4 digit random number, there is no way it could be guessed. It also generates a different random number each time ensuring that the OTP or PIN cannot be reused, memorized or misused. [3] The system sends the OTP as an SMS to the students registered Mobile Number or through college Wi-Fi in case there is no network. Once this OTP is entered by the student, he needs to be connected to college Wi-Fi to submit the OTP after tapping their tag on the student device. This extra measure ensures that students who are at home or outside the class won't be able to verify the OTP through their Student Application as their devices need to be connected to the institutions Wi-Fi and Tag needs to be inside Class. Those who have verified the OTP have also verified their presence in class as the device is connected to the Local Wi-Fi Network. The OTP method was proposed in order to make the system fool proof and prevent proxies. [12] What makes the system more secure is the OTP verification that takes place. Consider the student has swiped his tag against the sensor device and receives his OTP, there comes a scenario where if a student sends his tag with a colleague and forwards the SMS he received containing the OTP from home. Now the colleague can enter the OTP within the expiry time and the proxy attendance is marked. Therefore, to counter this, a feature was introduced which allowed OTP verification only when the Tag is in proximity of the students own mobile phone. This is possible because each student logs into the app on his/her device using their own credentials only. Hence, when we bring the Tag in proximity of the device the application recognizes that the tag number and credentials belong to the same person, hence the dual- verification takes place. Attendance is logged into the database as soon as the lecture ends.

VI. Experimental Results

a. Web Application

This section show the snapshot of web application.

The fig-a shows how the admin login in his server can view the attendance.

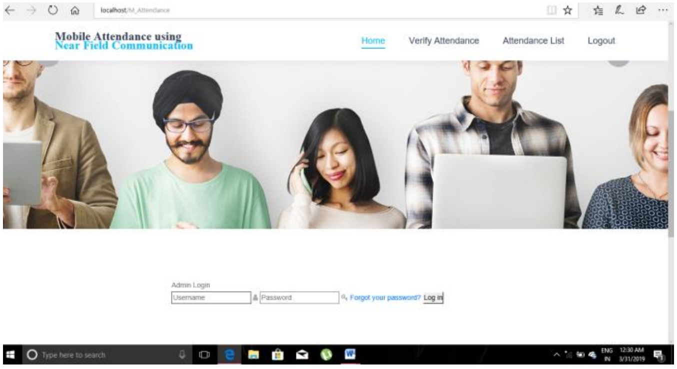
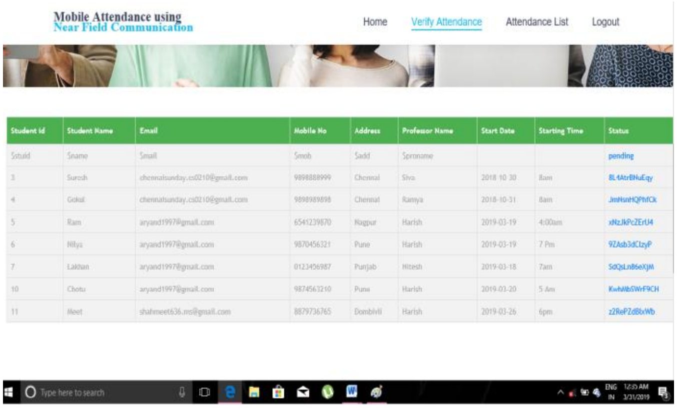


Fig-a Admin page

In this fig admin can view he attendance can verify the attendance by clicking it and OTP is send to student email ID.

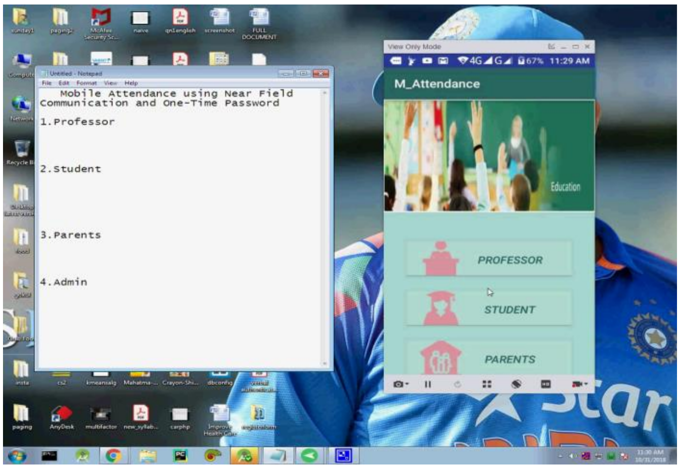


Student id	Student Name	Email	Mobile No	Address	Professor Name	Start Date	Starting Time	Status
$stuid	$name	$mail	$mob	$add	$proname			pending
3	Suresh	chennaisunday.cs0210@gmail.com	9898888999	Chennai	Siva	2018 10 30	8am	8L4AtrBNuEqy
4	Gokul	chennaisunday.cs0210@gmail.com	9898989898	Chennai	Ramya	2018-10-31	8am	JmNsnHQPhfCk
5	Ram	aryand1997@gmail.com	6541239870	Nagpur	Harish	2019-03-19	4:00am	xNzJkPcZErU4
6	Nilya	aryand1997@gmail.com	9870456321	Pune	Harish	2019-03-19	7 Pm	9ZAsb3dClzyP
7	Lakhan	aryand1997@gmail.com	0123456987	Punjab	Hitesh	2019-03-18	7am	SdQsLn86eXjM
10	Chotu	aryand1997@gmail.com	9874563210	Pune	Harish	2019-03-20	5 Am	KwhWbSWrF9CH
11	Meet	shahmeet636.ms@gmail.com	8879736765	Dombivli	Harish	2019-03-26	6pm	z2RePZdBbWb

Fig-b Attendance List

Android application

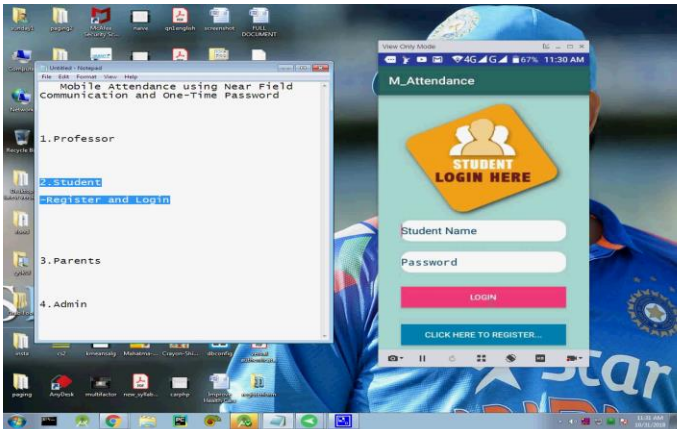
This fig .c shows the application view in the mobile device and that section login of student parents and professor.



```
   Mobile Attendance using Near Field
Communication and One-Time Password
1.Professor


2.Student



3.Parents


4.Admin
```

Fig-c User login page

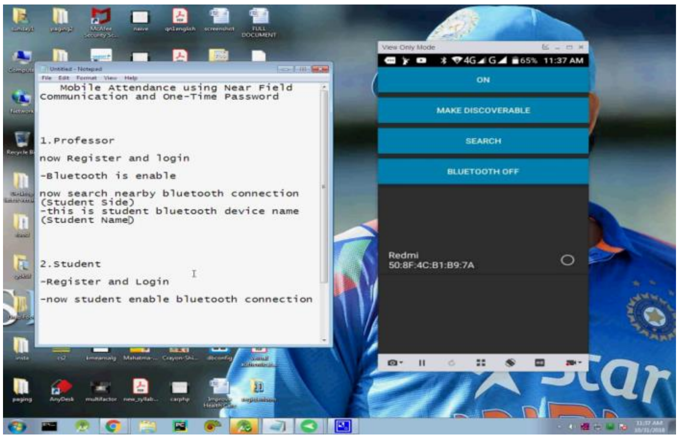
This fig-d shows the student login page in mobile device.



```
    Mobile Attendance using Near Field
Communication and One-Time Password


1.Professor


2.Student
-Register and Login


3.Parents


4.Admin
```

Fig-d Student login page

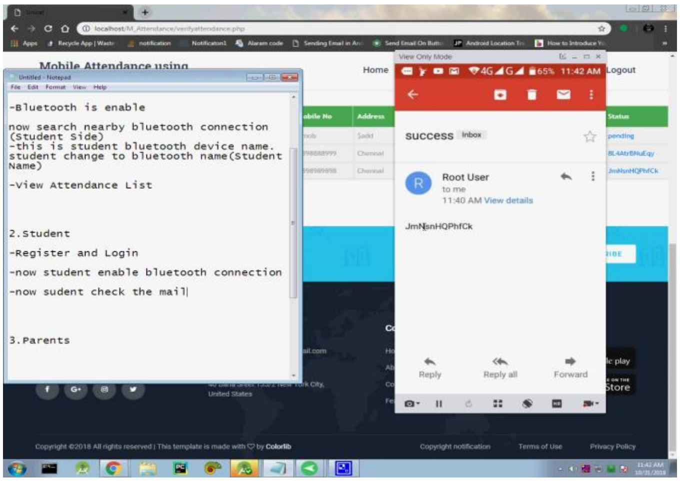
This fig-e shows the professor login page and which he make the Bluetooth discoverable for connection purpose.



```
    Mobile Attendance using Near Field
Communication and One-Time Password


1.Professor
now Register and login
-Bluetooth is enable
now search nearby bluetooth connection
(Student Side)
-this is student bluetooth device name
(Student Name)


2.Student
-Register and Login
-now student enable bluetooth connection
```

Fig-e Bluetooth connection page

This fig-f shows the OTP message send to the student device where he can enter OTP to login page to confirm his attendance .



```
-Bluetooth is enable
now search nearby bluetooth connection
(Student Side)
-this is student bluetooth device name.
student change to bluetooth name(Student
Name)
-View Attendance List


2.Student
-Register and Login
-now student enable bluetooth connection
-now sudent check the mail


3.Parents
```

success Inbox

Root User
to me
11:40 AM View details

JmNsnHQPhfCk

Fig-f Verification page

VII. CONCLUSIONS

The traditional attendance system have a tendency to be insecure due to absence of verification. In the proposed framework, we are utilizing Bluetooth and one time password for verification of employee and enlistment of participation in a systematic and secured way .Every student will be utilized along with mobile device which would be utilized for automating the way of marking attendance.

The mobile device attendance framework can reduce unnecessary manual work by enabling administrator to get real time information about attendance of an student. The advantages for the administrator are that to maintain all the data about employee attendance and keeping log record for future reference.

ACKNOWLEDGEMENT

This work was supported in part by Prof. Nilima Nikam, Mr. Ankit B Dubey, Mr. Ankit M Dubey, Mr. Nitesh Gupta We gratefully acknowledge the work of Tasgaonkar Institute of Engineering and Technology.

VIII. REFERENCES

1. Near Field Communication, White paper, ECMA international, December 2003

2. M. Viju Prakash, P. Alwin Infant, and S. Jeya Shobana, "Eliminating Vulnerable Attacks Using One-Time Password and Pass Text - Analytical Study of Blended Schema", Universal Journal of Computer Science and Engineering Technology 1 (2), 133-140, ISSN: 2219-2158, November 2010.

3. D. Florencio and C. Herley, "One-Time Password Access to Any Server without Changing the Server", Springer-Verlag, pp. 401-420, Berlin, Heidelberg, 2008.

4. Eamonn O'Neill, Peter Thompson, Stavros Garzonis, and Andrew Warr," Reach Out and Touch: Using NFC and 2D Barcodes for Service Discovery and Interaction with Mobile Devices", UK, 2007

5. MatijaBumbak," Analysis of potential RFID security problems in supply chains and ways to avoid them", Master thesis, May 2005

6. K. Preethi, A. Sinha, and Nandini, "Contactless Communication through Near Field Communication, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012, ISSN: 2277 128X

7. .https://en.wikipedia.org/wiki/Software_requirements_specification

8. P Elakiyaselvi, "A framework for implementing M-Attendance system using near field communication in android OS".

9. K. G. Paterson, and Douglas Stebila, "One-time-password authenticated key exchange" September 4, 2009.

10. T. Chang-Lung, C. Chun-Jung, and Z. Deng-Jie, "Secure OTP and Biometric Verification Scheme for Mobile Banking", Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing, IEEE, 2012.

11. T. Saini, "One Time Password Generator System", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, ISSN: 2277 128X, March 2014.

12. A. A. Khan, "Preventing Phishing Attacks using One Time Password and User Machine Identification", International Journal of Computer Applications (0975 - 8887),Volume 68-No. 3, April 2013.